The US-CERT Cyber Security Bulletin provides a summary of new and updated vulnerabilities, exploits, trends, and malicious code that have recently been openly reported. Information in the Cyber Security Bulletin is a compilation of open source and US-CERT vulnerability information. As such, the Cyber Security Bulletin includes information published by sources outside of US-CERT and *should **not** be considered the result of US-CERT analysis or as an official report of US-CERT*. Although this information does reflect open source reports, it is not an official description and should be used for informational purposes only. The intention of the Cyber Security Bulletin is to serve as a comprehensive directory of pertinent vulnerability reports, providing brief summaries and additional sources for further investigation.

Vulnerabilities

The tables below summarize vulnerabilities that have been reported by various open source organizations or presented in newsgroups and on web sites. **Items in bold designate updates that have been made to past entries.** Entries are grouped by the operating system on which the reported software operates, and vulnerabilities which affect both Windows and Unix/ Linux Operating Systems are included in the Multiple Operating Systems table. *Note*, entries in each table are not necessarily vulnerabilities *in* that operating system, but vulnerabilities in software which operate on some version of that operating system.

Entries may contain additional US-CERT sponsored information, including Common Vulnerabilities and Exposures (CVE) numbers, National Vulnerability Database (NVD) links, Common Vulnerability Scoring System (CVSS) values, Open Vulnerability and Assessment Language (OVAL) definitions, or links to US-CERT Vulnerability Notes. Metrics, values, and information included in the Cyber Security Bulletin which has been provided by other US-CERT sponsored programs, is prepared, managed, and contributed by those respective programs. CVSS values are managed and provided by the US-CERT/ NIST National Vulnerability Database. Links are also provided to patches and workarounds that have been provided by the product's vendor.

The Risk levels are defined below:

High - Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

Medium - Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.

Low - Vulnerabilities will be labeled "Low" severity if they have a CVSS base score of 0.0-3.9.

Note that scores provided prior to 11/9/2005 are approximated from only partially available CVSS metric data. Such scores are marked as "Approximated" within NVD. In particular, the following CVSS metrics are only partially available for these vulnerabilities and NVD assumes certain values based on an approximation algorithm: AccessComplexity, Authentication, ConfImpact of 'partial', IntegImpact of 'partial', AvailImpact of 'partial', and the impact biases.

Windows Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
BitComet Client 0.6	A buffer overflow vulnerability has been reported in BitComet Client that could let remote malicious users execute arbitrary code. BitComet 0.61 Currently we are not aware of any exploits for this vulnerability.	BitComet Client Arbitrary Code Execution CVE-2006-0339	7	Secunia, Advisory: SA18522, January 19, 2006
DM Deployment Common Component (DMPrimer) 1.4.154, 1.4.155	A vulnerability has been reported in DM Deployment Common Component (DMPrimer) that could let remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	DM Deployment Common Component (DMPrimer) Lets Remote Users Deny Service CVE-2006-0306	2.3	Security Tracker, Alert ID: 1015504, January 18, 2006
Hitachi JP1/ NetInsight II prior to 07-50-01	A vulnerability has been reported in JP1/ NetInsight II that could let remote malicious users cause a Denial of Service. A vendor solutions is available, contact Hitachi. Currently we are not aware of any exploits for this vulnerability.	Hitachi JP1/ NetInsight II Denial of Service CVE-2006-0343	2.3	Hitachi, HS05-025, January 20, 2006

Hitachi HITSENSER Data Mart Server prior to 01-06-/A	An input validation vulnerability has been reported in HITSENSER Data Mart Server that could let remote malicious users perform SQL injection. A vendor solutions is available, contact Hitachi. Currently we are not aware of any exploits for this vulnerability.	Hitachi HITSENSER Data Mart Server SQL Injection CVE-2006-0329	7	Hitachi, HS05-026, January 20, 2006
InterVations FileCOPA FTP Server 1.01 11-21-2005 release	An input validation vulnerability has been reported in FIleCOPA FTP Server that could let remote malicious users disclose information or obtain arbitrary file controls. FileCOPA 1.01 01-19-2006 release There is no exploit code required.	FileCOPA FTP Server Information Disclosure or Arbitrary File Control CVE-2006-0344	4.7	Secunia, Advisory: SA18550, January 20, 2006
Kerio WinRoute Firewall	Multiple vulnerabilities have been reported in WinRoute Firewall that could let remote malicious users cause a Denial of Service. Kerio WinRoute Firewall 6.1.4 P1 There is no exploit code required.	Kerio WinRoute Firewall Denial of Service CVE-2006-0335	2.3	Secunia, Advisory: SA18542, January 19, 2006
Rockliffe MailSite Email Server 7.0.3.1	Multiple vulnerabilities have been reported in MailSite Email Server that could let local malicious user to conduct cross site scripting or cause a denial of service. Rockliffe MailSite 6 Hotfix Rockliffe MailSite 7 Hotfix A Proof of Concept exploit has been published.	MailSite Cross Site Scripting or Denial of Service CVE-2006-0341 CVE-2006-0342	2.3 (CVE-2006-0341) 3.3 (CVE-2006-0342)	Secunia, Advisory: SA18551, January 20, 2006
Sami FTP Server 2.0.1	A buffer overflow vulnerability has been reported in Sami FTP Server that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. An exploit script, sami_ftp_poc.pl, has been published.	Sami FTP Server Arbitrary Code Execution	Not Available	Secunia, Advisory: SA18574, January 25, 2006

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
Clam Anti-Virus ClamAV 0.80 - 0.87.1, 0.75.1, 0.70, 0.68, 0.67, 0.65, 0.60, 0.51-0.54	A buffer overflow vulnerability has been reported when attempting to handle compressed UPX files due to an unspecified boundary error in "libclamav/upx.c, which could let a remote malicious user execute arbitrary code. ClamAV SuSE Trustix Gentoo Mandriva **Debian** Currently we are not aware of any exploits for this vulnerability.	ClamAV UPX File Handling CVE-2006-0162	**7**	Secunia Advisory: SA18379, January 10, 2006 US-CERT VU#385908 SUSE Security Summary Report, SUSE-SR:2006:001, January 13, 2006 Trustix Secure Linux Security Advisory, 2006-0002, January 13, 2006 Gentoo Linux Security Advisory, GLSA 200601-07, January 13, 2006 Mandriva Security Advisory, MDKSA-2006:016, January 16, 2006 **Debian Security Advisory, DSA-947-1, January 21, 2006**

Ecartis Ecartis 1.0.0 snapshot 20050909	A vulnerability has been reported when the PantoMIME functionality has been enabled because unauthorized users who are not subscribed to a mailing list can send email attachments that will be saved in the PantoMIME directory. No workaround or patch available at time of publishing. There is no exploit code required.	Ecartis PantoMIME Arbitrary Attachment Upload CVE-2006-0332	4.7	Secunia Advisory: SA18524, January 19, 2006
Edgewall Software Trac 0.9.1, 0.9, 0.8.1-0.8.4, 0.7.1	An SQL injection vulnerability has been reported in the search module due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrades available **Debian** There is no exploit code required; however, a Proof of Concept exploit has been published.	Edgewall Software Trac Search Module SQL Injection CVE-2005-4065	7	Security Focus, Bugtraq ID: 15720, December 5, 2005 **Debian Security Advisory, DSA-951-1, January 23, 2006**
Edgewall Software Trac 0.9.2	An HTML injection vulnerability has been reported in the WikiProcessor Wiki Content due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. Trac **Debian** There is no exploit code required.	Trac HTML Injection CVE-2005-4644	2.3	Security Focus, Bugtraq ID: 16198, January 10, 2006 **Debian Security Advisory, DSA-951-1, January 23, 2006**
Erik S. Raymond Fetchmail 6.3.0 - prior to 6.3.2	A remote Denial of Service vulnerability has been reported due to incorrect freeing of an invalid pointer when bouncing a message to the originator or to the local postmaster. Update available Currently we are not aware of any exploits for this vulnerability.	Fetchmail Remote Denial of Service CVE-2006-0321	2.3	Fetchmail Security Advisory, fetchmail-SA-2006-01, January 22, 2006
ETERM LibAST prior to 0.7	A buffer overflow vulnerability has been reported in 'conf.c' due to a boundary error in the 'conf_find_file()' function, which could let a malicious user execute arbitrary code. Update available An exploit script, eterm-exploit.c, has been published.	LibAST Buffer Overflow CVE-2006-0224	4.9	Secunia Advisory: SA18586, January 25, 2006
FreeBSD FreeBSD 5.3, 5.4, 6.0; OpenBSD 3.8, 3.7, OpenBSD -current	A remote Denial of Service vulnerability has been reported in the 'pf' Internet Protocol packet-filter fragment cache when handling IP fragments. Upgrade information There is no exploit code required.	FreeBSD Remote Denial of Service CVE-2006-0381	2.3	FreeBSD Security Advisory, FreeBSD-SA-06:07.pf, January 25, 2006
FreeBSD FreeBSD 6.0 -STABLE, 6.0 -RELEASE, 5.4 -RELENG, 5.4 -RELEASE, 5.4 -PRERELEASE	Several information disclosure vulnerabilities have been reported due to a failure of the kernel to properly clear previously used memory buffers prior to copying these buffers to user-space and too much data copied to user memory, which could let a remote malicious user obtain sensitive information. Update information There is no exploit code required.	FreeBSD Multiple Local Kernel Memory Disclosure CVE-2006-0379 CVE-2006-0380	1.6 (CVE-2006-0379) 1.6 (CVE-2006-0380)	FreeBSD Security Advisory, FreeBSD-SA-06:06.kmem, January 25, 2006
Hewlett Packard Company HP-UX 11.23, 11.11, 11.0 4, 11.0, B.11.23, B.11.11,	A remote Denial of Service vulnerability has been reported in the HP-UX ftpd implementation.	HP-UX FTPD Remote Denial of Service	2.3	HP Security Bulletin, HPSBUX02092, January 18, 2006

B.11.11, B.11.04, B.11.00	HP-UX There is no exploit code required.	CVE-2005-2993		
Image Magick ImageMagick 6.2.4 .5	A vulnerability has been reported in the delegate code that is used by various ImageMagick utilities when handling an image filename due to an error, which could let a remote malicious user execute arbitrary commands. **Ubuntu** There is no exploit code required.	ImageMagick Utilities Image Filename Remote Command Execution CVE-2005-4601	7	Secunia Advisory: SA18261, December 30, 2005 **Ubuntu Security Notice, USN-246-1, January 24, 2006**
KDE KDE 3.2.0 up to including 3.5.0	A buffer overflow vulnerability has been reported in 'kjs' in the decoding of UTF-8 encoded URI sequences, which could let a remote malicious user execute arbitrary code. Patch information RedHat Ubuntu Debian SuSE Mandriva Fedora Gentoo Currently we are not aware of any exploits for this vulnerability.	KDE kjs UTF-8 Encoded URI Buffer Overflow CVE-2006-0019	4.7	KDE Security Advisory, January 19, 2006 RedHat Security Advisory, RHSA-2006:0184-11, January 19, 2006 Ubuntu Security Notice, USN-245-1, January 20, 2006 Debian Security Advisory, DSA-948-1, January 20, 2006 SUSE Security Announcement, SUSE-SA:2006:003, January 20, 2006 Mandriva Security Advisory, MDKSA-2006:019, January 20, 2006 Gentoo Linux Security Advisory, GLSA 200601-11, January 22, 2006
Linley Henzel Crawl 4.0, BETA 26, BETA 23,	A vulnerability has been reported when saving and loading games due to the insecure execution of external programs, which could let a malicious user obtain elevated privileges. Debian There is no exploit code required.	Linley's Dungeon Crawl Arbitrary Command Execution CVE-2006-0045	4.9	Debian Security Advisory, DSA-949-1, January 20, 2006
LSH LSH 2.0.1	A vulnerability has been reported in 'unix_random.c' because file descriptors that are related to the randomness generator are leaked, which could let a malicious user obtain sensitive information or cause a Denial of Service. Patch available Currently we are not aware of any exploits for this vulnerability.	LSH File Descriptor Leakage CVE-2006-0353	3.3	Secunia Advisory: SA18564, January 23, 2006
Multiple Vendors Xpdf 3.0 pl2 & pl3, 3.0 1, 3.00, 2.0-2.03, 1.0 0, 1.0 0a, 0.90-0.93; RedHat Fedora Core4, Core3, Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, ES 2.1 IA64, 2.1, Enterprise Linux AS 4, AS 3, 2.1 IA64, 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1; teTeX 2.0.1, 2.0; Poppler poppler 0.4.2; KDE kpdf 0.5, KOffice 1.4.2 ; PDFTOHTML DFTOHTML 0.36	Multiple vulnerabilities have been reported: a heap-based buffer overflow vulnerability was reported in the 'DCTStream::read BaselineSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'DCTStream::read ProgressiveSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'StreamPredictor:: StreamPredictor()' function in 'xpdf/Stream.cc' when using the 'numComps' value to calculate the memory size, which could let a remote malicious user potentially execute	Xpdf Buffer Overflows CVE-2005-3191 CVE-2005-3192 CVE-2005-3193	**3.9** (CVE-2005-3191) 7 (CVE-2005-3192) **3.9** (CVE-2005-3193)	iDefense Security Advisory, December 5, 2005 Fedora Update Notifications, FEDORA-2005-1121 & 1122, December 6, 2005 RedHat Security Advisory, RHSA-2005:840-5, December 6, 2005 KDE Security Advisory, advisory-20051207-1, December 7, 2005 SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005 Ubuntu Security Notice, USN-227-1, December 12, 2005 Gentoo Linux Security

	arbitrary code; and a vulnerability was reported in the 'JPXStream: :readCodestream()' function in 'xpdf/JPXStream.cc' when using the 'nXTiles' and 'nYTiles' values from a PDF file to copy data from the file into allocated memory, which could let a remote malicious user potentially execute arbitrary code. Patches available Fedora RedHat KDE SUSE Ubuntu Gentoo RedHat RedHat RedHat Mandriva Debian Debian Debian Fedora **SuSE** **RedHat** **SGI** **Debian** Currently we are not aware of any exploits for these vulnerabilities.			Advisory, GLSA 200512-08, December 16, 2005 RedHat Security Advisories, RHSA-2005:868-4, RHSA-2005:867-5 & RHSA-2005:878-4, December 20, 2005 Mandriva Linux Security Advisories MDKSA-2006:003-003-006, January 6, 2006 Debian Security Advisory, DSA-936-1, January 11, 2006 Debian Security Advisory, DSA-937-1, January 12, 2006 Debian Security Advisory, DSA 938-1, January 12, 2006 Fedora Update Notifications, FEDORA-2005-028 & 029, January 12, 2006 SUSE Security Summary Report, SUSE-SR:2006:001, January 13, 2006 **RedHat Security Advisory, RHSA-2006:0160-14, January 19, 2006** **SUSE Security Summary Report, SUSE-SR:2006:002, January 20, 2006** **SGI Security Advisory, 20051201-01-U, January 20, 2006** **Debian Security Advisory, DSA-950-1, January 23, 2006**
Multiple Vendors Linux Kernel 2.4- 2.4.32	A Denial of Service vulnerability has been reported due to insufficient validation of the return code of a function call in the 'search_binary_handler()' function. Updates available RedHat A Proof of Concept exploit has been published.	Linux Kernel 'SEARCH_BINARY_HANDLER' Denial of Service CVE-2005-2708	2.3	Security Focus, Bugtraq ID: 16320, January 19, 2006 RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006
Multiple Vendors Linux kernel 2.6- 2.6.14	A Denial of Service vulnerability has been reported in 'net/ipv6/udp.c' due to an infinite loop error in the 'udp_v6_get_port()' function. Fedora Upgrades available Ubuntu SUSE **RedHat** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPV6 Denial of Service CVE-2005-2973	2.3	Secunia Advisory: SA17261, October 21, 2005 Fedora Update Notifications, FEDORA-2005-1007 & 1013, October 20, 2005 Security Focus, Bugtraq ID: 15156, October 31, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 **RedHat Security Advisory,**

				RHSA-2006:0140-9, January 19, 2006
Multiple Vendors Linux kernel 2.6-2.6.15	An integer overflow vulnerability has been reported in 'INVALIDATE_INODE_ PAGES2' which could lead to a Denial of Service and possibly execution of arbitrary code. Fedora **Mandriva** A Proof of Concept exploit script has been published.	Linux Kernel Integer Overflow CVE-2005-3808	3.5	Fedora Update Notification, FEDORA-2005-1138, December 13, 2005 **Mandriva Security Advisory, MDKSA-2006:018, January 20, 2006**
Multiple Vendors OpenSSH 3.x, 4.x; RedHat Fedora Core3 & Core4	A vulnerability has been reported in 'scp' when performing copy operations that use filenames due to the insecure use of the 'system()' function, which could let a malicious user obtain elevated privileges. Fedora There is no exploit code required.	OpenSSH SCP Shell Command Execution CVE-2006-0225	4.9	Security Focus, Bugtraq ID: 16369, January 24, 2006 Fedora Security Advisory, FEDORA-2006-056, January 24, 2006
Multiple Vendors SuSE Linux Professional 10.0 OSS, 10.0, Linux Personal 10.0 OSS; Linux kernel 2.6-2.6.15	A Denial of Service vulnerability has been reported due to a race condition in 'do_coredump'. SUSE **Mandriva** There is no exploit code required.	Linux Kernel do_coredump Denial of Service CVE-2005-3527	2.8	SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 **Mandriva Security Advisory, MDKSA-2006:018, January 20, 2006**
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Todd Miller Sudo 1.6-1.6.8, 1.5.6-1.5.9	A vulnerability has been reported in the 'PYTHONINSPECT' variable, which could let a malicious user bypass security restrictions and obtain elevated privileges. Todd Miller Sudo AppleWebSharing Update Conectiva Debian EnGarde Fedora FreeBSD GratiSoft Sudo Mandriva OpenPKG OpenBSD RedHat Slackware SuSE Trustix TurboLinux Ubuntu Wirex **Debian** **SuSE** An exploit script, sudo_local_python_	Sudo Python Environment Cleaning Security Bypass CVE-2006-0151	7	Security Focus, Bugtraq ID: 16184, January 9, 2006 Security Focus, Bugtraq ID: 16184, January 12, 2006 **Debian Security Advisory, DSA-946-1, January 20, 2006** **SUSE Security Summary Report, SUSE-SR:2006:002, January 20, 2006**

	exploit.txt, has been published.			
Multiple Vendors KDE kword 1.4.2, kpdf 3.4.3, 3.2, KOffice 1.4-1.4.2, kdegraphics 3.4.3, 3.2; Gentoo Linux	Multiple buffer and integer overflows have been reported, which could let a remote malicious user execute arbitrary code. Gentoo Ubuntu Fedora Mandriva Ubuntu Debian Debian SuSE RedHat RedHat Fedora Debian Trustix Mandriva **RedHat** **SGI** **Debian** Currently we are not aware of any exploits for this vulnerability.	KPdf & KWord Multiple Unspecified Buffer & Integer Overflow CVE-2005-3624 CVE-2005-3625 CVE-2005-3626 CVE-2005-3627	Not Available	Gentoo Linux Security Advisory GLSA 200601-02, January 5, 2006 Ubuntu Security Notice, USN-236-1, January 05, 2006 Fedora Update Notifications, FEDORA-2005-000, January 5, 2006 Mandriva Linux Security Advisories MDKSA-2006:003-003-006 & 008, January 6 & 7, 2006 Ubuntu Security Notice, USN-236-2, January 09, 2006 Debian Security Advisory DSA 931-1, January 9, 2006 Debian Security Advisory, DSA-936-1, January 11, 2006 SUSE Security Announcement, SUSE-SA:2006:001, January 11, 2006 RedHat Security Advisories, RHSA-2006:0163-2 & RHSA-2006:0177-5, January 11, 2006 Fedora Update Notifications, FEDORA-2005-028 & 029, January 12, 2006 Debian Security Advisories, DSA 937-1, 938-1, & 940-1, January 12 & 13, 2006 Trustix Secure Linux Security Advisory, 2006-0002, January 13, 2006 Mandriva Linux Security Advisory, MDKSA-2006:012, January 13, 2006 **RedHat Security Advisory, RHSA-2006:0160-14, January 19, 2006** **SGI Security Advisory, 20051201-01-U, January 20, 2006** **Debian Security Advisory, DSA-950-1, January 23, 2006**
Multiple Vendors Linux kernel 2.6-2.6.12, 2.4-2.4.31	A remote Denial of Service vulnerability has been reported due to a design error in the kernel. The vendor has released versions 2.6.13 and 2.4.32-rc1 of the kernel to address this issue. Ubuntu Mandriva SUSE Conectiva **RedHat** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Remote Denial of Service CVE-2005-3275	3.3	Ubuntu Security Notice, USN-219-1, November 22, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 **RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006**

Multiple Vendors Linux kernel 2.6-2.6.13.1	A Denial of Service vulnerability has been reported due to an omitted call to the 'sockfd_put()' function in the 32-bit compatible 'routing_ioctl()' function. Linux Kernel Ubuntu Mandriva SUSE Conectiva RedHat **RedHat** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel routing_ioctl() Denial of Service CVE-2005-3044	2.3	Security Tracker Alert ID: 1014944, September 21, 2005 Ubuntu Security Notice, USN-187-1, September 25, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219, 220, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 **RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006**
Multiple Vendors Linux kernel 2.6-2.6.14	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to a memory leak in '/security/keys/request_key_auth.c;' a Denial of Service vulnerability was reported due to a memory leak in '/fs/namei.c' when the 'CONFIG_AUDITSYSCALL' option is enabled; and a vulnerability was reported because the orinoco wireless driver fails to pad data packets with zeroes when increasing the length, which could let a malicious user obtain sensitive information. Linux Kernel Fedora Trustix RedHat Ubuntu Mandriva SUSE Conectiva **RedHat** There is no exploit code required.	Linux Kernel Denial of Service & Information Disclosure CVE-2005-3119 CVE-2005-3180 CVE-2005-3181	2.3 (CVE-2005-3119) 3.3 (CVE-2005-3180) 2.3 (CVE-2005-3181)	Secunia Advisory: SA17114, October 12, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0057, October 14, 2005 Fedora Update Notifications, FEDORA-2005-1013, October 20, 2005 RedHat Security Advisory, RHSA-2005:808-14, October 27, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 **RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006**
Multiple Vendors Linux kernel 2.6-2.6.14	A Denial of Service vulnerability has been in 'sysctl.c' due to an error when handling the un-registration of interfaces in '/proc/sys/net/ipv4/conf/.' Upgrades available Ubuntu RedHat	Linux Kernel 'Sysctl' Denial of Service CVE-2005-2709	**4.9**	Secunia Advisory: SA17504, November 9, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006

	RedHat There is no exploit code required.			**RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006**

Multiple Vendors
Linux kernel 2.6-2.6.14;
SuSE Linux Professional 10.0 OSS, Linux Personal 10.0 OSS;
RedHat Fedora Core4
	A Denial of Service vulnerability has been reported in 'ptrace.c' when 'CLONE_THREAD' is used due to a missing check of the thread's group ID when trying to determine whether the process is attempting to attach to itself.
	Upgrades available
	Fedora
	SUSE
	Mandriva
	Currently we are not aware of any exploits for this vulnerability.
		Linux Kernel PTrace 'CLONE_ THREAD' Denial of Service
		CVE-2005-3783
			3.5	Secunia Advisory: SA17761, November 29, 2005
				Fedora Update Notification, FEDORA-2005-1104, November 28, 2005
				SuSE Security Announcement, SUSE-SA:2005:067, December 6, 2005
				SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005
				Mandriva Security Advisory, MDKSA-2006:018, January 20, 2006

Multiple Vendors Linux kernel 2.6-2.6.15	A Denial of Service vulnerability has been reported in the 'time_out_leases()' function because 'printk()' can consume large amounts of kernel log space. Patches available Trustix RedHat **RedHat** An exploit script has been published.	Linux Kernel PrintK Local Denial of Service CVE-2005-3857	3.5	Security Focus, Bugtraq ID: 15627, November 29, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0070, December 9, 2005 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 **RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006**

Multiple Vendors
Linux kernel 2.6-2.6.15;
SuSE Linux Professional 10.0 OSS, Linux Personal 10.0 OSS;
RedHat Fedora Core4
	A Denial of Service vulnerability has been reported because processes are improperly auto-reaped when they are being ptraced.
	Patches available
	Fedora
	Trustix
	SUSE
	RedHat
	Mandriva
	Currently we are not aware of any exploits for this vulnerability.
		Linux Kernel PTraced Denial of Service
		CVE-2005-3784
			3.5	Security Focus, Bugtraq ID: 15625, November 29, 2005
				Fedora Update Notification, FEDORA-2005-1104, November 28, 2005
				SuSE Security Announcement, SUSE-SA:2005:067, December 6, 2005
				Trustix Secure Linux Security Advisory, TSLSA-2005-0070, December 9, 2005
				SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005
				RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006
				Mandriva Security Advisory, MDKSA-2006:018, January 20, 2006

Multiple Vendors SuSE Linux Professional 10.0 OSS, 10.0 OSS; Linux kernel 2.6.10 -2.6.14	A Denial of Service vulnerability has been reported due to a race condition error in the handling of POSIX timer cleanup routines. Linux kernel versions subsequent to 2.6.14 are not vulnerable to this issue. SUSE **Mandriva** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel POSIX Timer Cleanup Handling Local Denial of Service CVE-2005-3805	3.5	SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 **Mandriva Security Advisory, MDKSA-2006:018, January 20, 2006**
Multiple Vendors SuSE Linux Professional 10.0 OSS, 10.0, Personal	A Denial of Service vulnerability has been reported in FlowLable. Upgrades available	Linux Kernel IPv6 FlowLable Denial of Service	5.3	Security Focus, Bugtraq ID: 15729, December 6, 2005 SUSE Security

10.0 OSS; Linux kernel 2.6-2.6.13, Linux kernel 2.4-2.4.32	SUSE RedHat **RedHat** **Mandriva** Currently we are not aware of any exploits for this vulnerability.	CVE-2005-3806		Announcement, SUSE-SA:2005:067, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 **RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006** **Mandriva Security Advisory, MDKSA-2006:018, January 20, 2006**
Multiple Vendors Ubuntu Linux 4.1 ppc, ia64, ia32; Linux kernel 2.6-2.6.10, 2.4-2.4.28	A vulnerability has been reported in the SDLA driver, which could let a malicious user obtain unauthorized access. Updates available Ubuntu Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SDLA IOCTL Unauthorized Local Firmware Access CVE-2006-0096	4.9	Ubuntu Security Notice, USN-244-1 January 18, 2006

Multiple Vendors
Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32;
IBM HTTP Server 2.0.47.1, 2.0.47, 2.0.42.2, 2.0.42.1, 2.0.42;
Apache 2.0.28-2.0.54, 2.0 a9, 2.0
	A remote Denial of Service vulnerability has been reported in 'worker.c' due to a memory leak.
	Apache
	Ubuntu
	IBM
	RedHat
	Fedora
	There is no exploit code required.
		Apache MPM 'Worker.C' Remote Denial of Service
		CVE-2005-2970
			3.3	Security Focus, Bugtraq ID: 15762, December 7, 2005
				Ubuntu Security Notice, USN-225-1, December 06, 2005
				RedHat Security Advisory, RHSA-2006:0159-8, January 5, 2006
				Fedora Security Advisory, FEDORA-2006-052, January 23, 2006

Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6-2.6.15	A vulnerability has been reported in the 'cm-crypt' driver due to a failure to clear memory, which could let a malicious user obtain sensitive information. Updates available Ubuntu Currently we are not aware of any exploits for this vulnerability.	Linux Kernel DM-Crypt Local Information Disclosure CVE-2006-0095	1.6	Security Focus, Bugtraq ID: 16301, January 18, 2006 Ubuntu Security Notice, USN-244-1 January 18, 2006
MyDNS MyDNS 1.0.0	A remote Denial of Service vulnerability has been reported due to an error when handling certain malformed DNS queries. Update available Currently we are not aware of any exploits for this vulnerability.	MyDNS Remote Denial of Service CVE-2006-0351	3.3	Security Tracker Alert ID: 1015521, January 20, 2006
Sun Microsystems, Inc. Sun Grid Engine (SGE) prior to 6.0u7_1	A vulnerability has been reported in 'utilbin/<arch>/rsh' due to an error, which could let a malicious user obtain elevated privileges or execute arbitrary code. Update available Currently we are not aware of any exploits for this vulnerability.	Sun Grid Engine Elevated Privileges CVE-2006-0408	7	Security Tracker Alert ID: 1015531, January 24, 2006
Todd Miller Sudo 1.x	A vulnerability has been reported in the environment cleaning due to insufficient sanitization, which could let a malicious user obtain elevated privileges. Debian	Todd Miller Sudo Local Elevated Privileges CVE-2005-2959	4.9	Debian Security Advisory, DSA 870-1, October 25, 2005 Mandriva Linux Security Advisory, MDKSA-2005:201, October 27, 2005 Ubuntu Security Notice,

	Mandriva Ubuntu SUSE Trustix Conectiva **SuSE** An exploit script has been published.			USN-213-1, October 28, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Security Focus, Bugtraq ID: 15191, November 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0062, November 22, 2005 Conectiva Linux Announcement, CLSA-2006:1057, January 2, 2006 **SUSE Security Summary Report, SUSE-SR:2006:002, January 20, 2006**
Todd Miller Sudo prior to 1.6.8p12	A vulnerability has been reported due to an error when handling the 'PERLLIB,' 'PERL5LIB,' and 'PERL5OPT' environment variables when tainting is ignored, which could let a malicious user bypass security restrictions and include arbitrary library files. Sudo Mandriva Ubuntu Trustix **Debian** **SuSE** There is no exploit code required; however, a Proof of Concept exploit script has been published.	Todd Miller Sudo Security Bypass CVE-2005-4158	4.9	Security Focus, Bugtraq ID: 15394, November 11, 2005 Mandriva Linux Security Advisory, MDKSA-2005:234, December 20, 2005 Ubuntu Security Notice, USN-235-1, January 05, 2006 Trustix Secure Linux Security Advisory, 2006-0002, January 13, 2006 **Debian Security Advisory, DSA-946-1, January 20, 2006** **SUSE Security Summary Report, SUSE-SR:2006:002, January 20, 2006**

University of Washington UW-imapd imap-2004c1	A buffer overflow has been reported in UW-imapd that could let remote malicious users cause a Denial of Service or execute arbitrary code. Upgrade to version imap-2004g Trustix Debian Gentoo SUSE Mandriva Slackware Conectiva RedHat RedHat Fedora Trustix **SGI** Currently we are not aware of any exploits for this vulnerability.	UW-imapd Denial of Service and Arbitrary Code Execution CVE-2005-2933	7	Secunia, Advisory: SA17062, October 5, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0055, October 7, 2005 Debian Security Advisory, DSA 861-1, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-10, October 11, 2005 US-CERT VU#933601 SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:189 & 194, October 21 & 26, 2005 Slackware Security Advisory, SSA:2005-310-06, November 7, 2005 Conectiva Linux Announcement, CLSA-2005:1046, November 21, 2005 RedHat Security Advisory, RHSA-2005:848-6 & 850-5, December 6, 2005 Fedora Update Notifications, FEDORA-2005-1112 & 1115, December 8, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0074, December 23, 2005 **SGI Security Advisory, 20051201-01-U, January 20, 2006**
WeBWorK WebWorK Online Homework Delivery System 2.1.3	A vulnerability has been reported due to an unspecified error, which could let a remote malicious user execute arbitrary commands. Update available Currently we are not aware of any exploits for this vulnerability.	WeBWorK Remote Arbitrary Command Execution	Not Available	Secunia Advisory: SA18594, January 25, 2006

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Description	Common Name	CVSS	Resources
3Com TippingPoint IPS TOS	A remote Denial of Service vulnerability has been reported due to an error in TOS (TippingPoint OS) when handling certain HTTP traffic. Contact the vendor for information on obtaining fixes. There is no exploit code required.	TippingPoint IPS Device Remote Denial of Service CVE-2006-0362	2.3	Secunia Advisory: SA18515, January 19, 2006
ADOdb ADOdb 4.70, 4.68, 4.66	An SQL injection vulnerability has been reported due to insufficient sanitization of certain parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Updates available	ADOdb PostgreSQL SQL Injection CVE-2006-0410	2.3	Secunia Advisory: SA18575, January 24, 2006

	There is no exploit code required.			
Ahmad Text Rider 2.4	A vulnerability has been reported in the 'data/userlist.txt' file due to insufficient protection, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Text Rider Information Disclosure	Not Available	Security Tracker Alert ID: 1015533, January 24, 2006
Apache Software Foundation Apache prior to 1.3.35-dev, 2.0.56-dev	A Cross-Site Scripting vulnerability has been reported in the 'Referer' directive in 'mod_imap' due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. The vulnerability has been fixed in version 1.3.35-dev, and 2.0.56-dev. OpenPKG Trustix Mandriva Ubuntu RedHat **Fedora** There is no exploit code required.	Apache mod_imap Cross-Site Scripting CVE-2005-3352	2.3	Security Tracker Alert ID: 1015344, December 13, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.029, December 14, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0074, December 23, 2005 Mandriva Linux Security Advisory, MDKSA-2006:007, January 6, 2006 Ubuntu Security Notice, USN-241-1, January 12, 2006 RedHat Security Advisory, RHSA-2006:0158-4, January 17, 2006 **Fedora Security Advisory, FEDORA-2006-052, January 23, 2006**
AZ Bulletin Board AZbb 1.0-1.0.8	A Cross-Site Scripting vulnerability has been reported in 'post.php' due to insufficient sanitization of the 'topic' and 'nickname' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	AZ Bulletin Board Cross-Site Scripting CVE-2006-0407	2.3	KAPDA Advisory January 22, 2006
BEA Systems, Inc. WebLogic Express 6.x, 7.x, 8.x, 9.x, WebLogic Server 6.x, 7.x, 8.x, 9.x	Several vulnerabilities have been reported: a vulnerability was reported in the MBean protection due to an error, which could let a remote malicious user access protected MBean attributes or cause a Denial of Service; a vulnerability was reported due to insufficient protection of the server log, which could let a remote malicious user obtain sensitive information; a vulnerability was reported in the 'DefaultAuditRecorder.log' file when a password change occurs, because the WebLogic Auditing provider writes the old and new password in clear-text, which could let a remote malicious user obtain sensitive information; a vulnerability was reported due to insufficient protection of system passwords, which could let a remote malicious user obtain sensitive information; a vulnerability was reported because a new configured security provider is not activated until the server reboots, which could let a remote malicious user add/remove security policies and users; a vulnerability was reported because the usage of connection filters in certain situations cause the server	BEA WebLogic Server/Express Vulnerabilities CVE-2006-0422 CVE-2006-0424 CVE-2006-0426 CVE-2006-0427 CVE-2006-0429 CVE-2006-0430 CVE-2006-0431 CVE-2006-0432	4.7 (CVE-2006-0422) 1.4 (CVE-2006-0424) 7 (CVE-2006-0426) 1.6 (CVE-2006-0427) 4.9 (CVE-2006-0429) 2.3 (CVE-2006-0430) 1.6 (CVE-2006-0431) 1.6 (CVE-2006-0432)	BEA System Security Advisories, BEA06-109.00, BEA06-111.00, BEA06-113.00, BEA06-114.00, BEA06-116.00, BEA06-117.00, BEA06-118.00, & BEA06-119.00, January 23, 2006

	performance to decrease; a vulnerability was reported due to an error in the protection of the server's SSL identity, which could lead to the disclosure of sensitive information; and a vulnerability was reported because certain security policies added via the console by the administrator do not properly protect JNDI resources, which could let a remote malicious user obtain access certain restricted resources. Patch Information Currently we are not aware of any exploits for these vulnerabilities.			
BEA Systems, Inc. WebLogic Portal 8.x	Several vulnerabilities have been reported: a vulnerability was reported in the 'config.xml' file because database passwords are stored in clear-text, which could let a remote malicious user obtain sensitive information; a vulnerability was reported due to insufficient protection of the file source of an application's deployment descriptor, which could let a remote malicious user obtain sensitive information; and an input validation vulnerability was reported in WSRP (Web Services Remote Portlets), which could let a remote malicious user bypass security restrictions. Updates available Currently we are not aware of any exploits for these vulnerabilities.	BEA WebLogic Portal Information Disclosure & Security Bypass CVE-2006-0423 CVE-2006-0425 CVE-2006-0428	7 (CVE-2006-0423) 2.3 (CVE-2006-0425) 7 (CVE-2006-0428)	BEA System Security Advisories, BEA06-110.00, BEA06-112.00, & BEA06-115.00, January 23, 2006
BEA Systems, Inc. WebLogic Express 6.x, 7.x, WebLogic Server 6.x, 7.x	A vulnerability has been reported because an administrative user for a specific domain can access other domains if the same WebLogic Server instance and machine was used to create the domains. Update information Currently we are not aware of any exploits for this vulnerability.	BEA WebLogic Server/Express Multiple Domains Administrator Access CVE-2006-0421	4.9	BEA Systems Security Advisory, BEA06-108.00, January 23, 2006
Cisco Systems IOS 12.x, R12.x	A remote Denial of Service vulnerability has been reported due to an error in the handling of the SGBP protocol (Stack Group Bidding Protocol. Update & workaround Currently we are not aware of any exploits for this vulnerability.	Cisco IOS SGBP Remote Denial of Service CVE-2006-0340	1.4	Cisco Security Advisory, cisco-sa-20060118-sgbp, January 18, 2006
Claroline Claroline 1.7.2.	A vulnerability has been reported in the 'claro_init_local.inc.php' script because a predictable value is generated, which could let a remote malicious user bypass security restrictions. No workaround or patch available at time of publishing. There is no exploit code required.	Claroline E-Learning Session Hijacking CVE-2006-0411	7	Secunia Advisory: SA18588, January 25, 2006
Dave Carrigan auth_ldap 1.6 .0, 1.4 .x, 1.3 .x, 1.2 .x	A format string vulnerability has been reported due to insufficient sanitization of user-supplied input before using in the format-specifier of a formatted printing function, which could let a remote malicious user execute arbitrary code. Upgrade available RedHat **Mandriva** **Debian** Currently we are not aware of any exploits for this vulnerability.	Dave Carrigan Auth_LDAP Remote Format String CVE-2006-0150	**7**	Security Focus, Bugtraq ID: 16177, January 9, 2006 RedHat Security Advisory, RHSA-2006:0179-7, January 10, 2006 **Mandriva Security Advisory, MDKSA-2006:017, January 19, 2006** **Debian Security Advisory, DSA-952-1, January 23, 2006**

Douran Portal FollowWeb	A Cross-Site Scripting vulnerability has been reported in 'Register.ASPX' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Douran FollowWeb Portal Cross-Site Scripting CVE-2006-0373	2.3	Security Focus, Bugtraq ID: 16302, January 18, 2006
Elog Web Logbook Elog Web Logbook 2.6 .0, 2.5.7, 2.5.6, 2.5, 2.4, 2.2.0-2.2.4, 2.1.0-2.1.3, 2.0.0- 2.0.5	Multiple remote vulnerabilities have been reported including a format string vulnerability in the 'write_logfile()' function and a Directory Traversal vulnerability, which could lead to the execution of arbitrary code or access to sensitive information. Updates available Currently we are not aware of any exploits for these vulnerabilities.	ELOG Web Logbook Multiple Remote Input Validation CVE-2006-0347 CVE-2006-0348	2.3 (CVE-2006-0347) 3.3 (CVE-2006-0348)	Security Focus, Bugtraq ID: 16315, January 19, 2006
e-moBLOG e-moBLOG 1.3	SQL Injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of the 'monthy' parameter and in 'admin/index.php' due to insufficient sanitization of the 'login' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	e-moBLOG SQL Injection CVE-2006-0403	7	Secunia Advisory: SA18567, January 23, 2006
Epic Designs Eggblog 2.0	Several input validation vulnerabilities have been reported: an SQL injection vulnerability was reported in 'blog.php' due to insufficient sanitization of the 'id' parameter, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in the 'topic.php' script due to insufficient filtering of HTML code from user-supplied input in the message before displaying, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Eggblog Multiple Input Validation CVE-2006-0349 CVE-2006-0350	7 (CVE-2006-0349) 2.3 (CVE-2006-0350)	Security Tracker Alert ID: 1015505, January 18, 2006
Etomite Etomite 0.6	A vulnerability has been reported in 'manager/includes/todo.inc.php' due to the existence of a backdoor, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	Etomite Backdoor CVE-2006-0325	7	Secunia Advisory: SA18556, January 23, 2006
Flyspray Flyspray 0.9.8 development, 0.9.8, 0.9.7	Cross-Site Scripting vulnerabilities have been reported in 'index.php' due to insufficient sanitization of input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. **Debian** There is no exploit code required; however, Proof of Concept exploit URLs have been published.	Flyspray Multiple Cross-Site Scripting CVE-2005-3334	3.3	Flyspray Security Advisory, FS#703, October 24, 2005 **Debian Security Advisory, DSA-953-1, January 24, 2006**
F-Secure Anti-Virus 2004, 2005, 2006, Anti-Virus 5.x, Anti-Virus Client Security 5.x, 6.x, Anti-Virus for Citrix	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported when handling ZIP archives due to a boundary error, which could let a remote malicious user execute arbitrary code; and a	F-Secure Multiple Archive Handling CVE-2006-0337	7 (CVE-2006-0337) 10	F-Secure Security Bulletin FSC-2006-1, January 19, 2006

Servers 5.x, Anti-Virus for Firewalls 6.x, Anti-Virus for Linux 4.x, Anti-Virus for Microsoft Exchange 6.x, Anti-Virus for MIMEsweeper 5.x, Anti-Virus for Samba Servers 4.x, Anti-Virus for Windows Servers 5.x, Anti-Virus for Workstations 5.x, Internet Gatekeeper 6.x, Internet Gatekeeper for Linux 2.x, Internet Security 2004, 2005, 2006, Personal Express 6.x	vulnerability was reported in the scanning functionality when processing RAR and ZIP archives, which could prevent malware from detection. Patch Information Currently we are not aware of any exploits for these vulnerabilities.	CVE-2006-0338	(CVE-2006-0338)	
Gallery Project Gallery 1.5.2-RC2	An HTML injection vulnerability has been reported due to insufficient sanitization of the user's fullname before using, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Gallery HTML Injection CVE-2006-0330	2.3	Secunia Advisory: SA18557, January 20, 2006
Linksys BEFVP41 1.42.7, 1.40.4, 1.40.3f	A remote Denial of Service vulnerability has been reported due to an error in the handling of specially crafted IP packets that have the IP option length set to zero. No workaround or patch available at time of publishing. There is no exploit code required.	Linksys BEFVP41 IP Options Remote Denial of Service CVE-2006-0309	1.4	Security Tracker Alert ID: 1015490, January 16, 2006
miniBloggie miniBloggie 1.0 & prior	An SQL injection vulnerability has been reported in 'Login.PHP' due to insufficient sanitization of the username and password parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	miniBloggie SQL Injection CVE-2006-0417	7	Security Tracker Alert ID: 1015534, January 24, 2006

Multiple Vendors
BrightStor ARCserve Backup 11.x, ARCserve Backup 11.x (for Windows), ARCserve Backup 9.x, ARCserve Backup for Laptops & Desktops 11.x, Enterprise Backup 10.x, Process Automation Manager 11.x, Storage Resource Manager 11.x, 6.x;
CA Advantage Data Transformer 2.x, AllFusion Harvest Change Manager 7.x, BrightStor Portal 11.x, BrightStor SAN Manager 11.x, eTrust Admin 8.x, eTrust Audit 1.x, 8.x, eTrust Identity Minder 8.x, Unicenter Service Fulfillment 2.x;
eTrust Secure Content Manager (SCM); RedHat openssh-clients-3.9p1-8.0.1.i386.rpm 8.1;
Linux kernel-x86_64 9.01
	A buffer overflow vulnerability has been reported when handling HTTP data in the iGateway component due to a boundary error, which could let a remote malicious user execute arbitrary code.
	Updates available
	Currently we are not aware of any exploits for this vulnerability.
		CA Products iGateway Service Content-Length Buffer Overflow
		CVE-2005-3653
			7	iDefense Security Advisory, January 23, 2006

Multiple Vendors
RedHat openssh-server-3.9p1-8.0.1.i386.rpm 7.1;
Netscape Directory Server 6.21, 6.11, 6.2, 6.1, 6.0-6.0 2, 4.11-4.13, 4.1, 3.12, 3.1 P1, 1.3 P5;
Darryl Burgdorf Webhints 7.1
	A buffer overflow vulnerability has been reported in the Admin pages of the Management Console, which could let a remote malicious user execute arbitrary code.
	RedHat
	Currently we are not aware of any exploits for this vulnerability.
		Red Hat Directory Server / Certificate Server Management Console Buffer Overflow	Not Available	Security Focus, Bugtraq ID: 16345, January 23, 2006

MyBB Group MyBulletinBoard 1.0.2	An HTML injection vulnerability has been reported which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	MyBB Signature HTML Injection CVE-2006-0364	2.3	Security Focus, Bugtraq ID: 16308, January 18, 2006
MyBB Group MyBulletinBoard 1.0.2, 1.0.1	An HTML injection vulnerability has been reported due to insufficient validity checks on HTTP POST requests, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	MyBB HTML Injection	Not Available	KAPDA Advisory, January 21, 2006
Netrix X-Site Manager	A Cross-Site Scripting vulnerability has been reported in 'Product_Details.PHP' due to insufficient sanitization of the 'product_id' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Netrix X-Site Manager Cross-Site Scripting CVE-2006-0378	2.3	Secunia Advisory: SA18537, January 19, 2006
newsPHP newsPHP	SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	NewsPHP Multiple SQL Injection CVE-2006-0413	7	Security Focus, Bugtraq ID: 16339, January 23, 2006
Noah Medling RCBlog 1.03	Several vulnerabilities have been reported: a vulnerability was reported in the 'data' and 'config' directories because user information is stored in textfiles, which could let a remote malicious user obtain sensitive information; a Directory Traversal vulnerability was reported in 'index.php' due to insufficient verification of the 'post' parameter before used to view files, which could let a remote malicious user obtain sensitive information; and a vulnerability was reported because administrators can upload arbitrary files to a location inside the web root, which could lead to the execution of arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	RCBlog File Upload & Information Disclosure CVE-2006-0370 CVE-2006-0371	2.3 (CVE-2006-0370) 2.3 (CVE-2006-0371)	Secunia Advisory: SA18547, January 20, 2006
Oracle Corporation JD Edwards EnterpriseOne 8.x, Oracle Application Server 10g, Collaboration Suite Release 1 & Release 2, Database 8.x, Database Server 10g, Developer Suite 10g, E-Business Suite 11i, Enterprise Manager 10.x, Oracle9i Application Server, Oracle9i Database Enterprise Edition, Oracle9i Database Standard Edition, Oracle9i Developer Suite, PeopleSoft Enterprise Portal 8.x	82 vulnerabilities and security issues have been reported in various Oracle products, which could lead to information disclosure, arbitrary files overwritten, and arbitrary SQL code injection. patch information An exploit would not be required for some of these issues.	Oracle January Security Update CVE-2005-2371 CVE-2005-2378 CVE-2006-0256 through CVE-2006-0291	3.3 (CVE-2005-2371) 3.3 (CVE-2005-2378) 7 (CVE-2006-0256 through CVE-2006-0271) 7 (CVE-2006-0272 through CVE-2006-0278)	Security Focus, Bugtraq ID: 16287, January 17, 2006 US-CERT VU#545804 Technical Cyber Security Alert TA06-018A **US-CERT VU#472148** **US-CERT VU#925261** **US-CERT VU#857412** **US-CERT VU#871756**

			4.9 (CVE-2006-0279 & CVE-2006-0280) 7 (CVE-2006-0281 through CVE-2006-0291)	**US-CERT VU#999268** **US-CERT VU#629316** **US-CERT VU#983340** **US-CERT VU#150332** **US-CERT VU#891644** **US-CERT VU#870172**
PhlyLabs PHlyMail 3.0.2 .01, 3.0.2 .00	Several input validation vulnerabilities have been reported: a vulnerability was reported due to insufficient sanitization of unspecified input before using, which could let a remote malicious user execute arbitrary JavaScript code; and an SQL injection vulnerability was reported due to insufficient sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Users are advised to contact the vendor for details on obtaining the appropriate updates. There is no exploit code required.	PHlyMail Multiple Input Validation CVE-2005-4652 CVE-2005-4666	4.7 (CVE-2005-4652) 2.3 (CVE-2005-4666)	Security Focus, Bugtraq ID: 16310, January 19, 2006
Pixelpost Pixelpost 1.4.3.	An HTML injection vulnerability has been reported due to insufficient sanitization of user comments, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Pixelpost HTML Injection CVE-2006-0409	2.3	Secunia Advisory: SA18572, January 24, 2006
saralblog saralblog 1.0	Multiple input validation vulnerabilities have been reported due to insufficient sanitization of unspecified user-supplied input, which could let a remote malicious user execute arbitrary SQL code, HTML, or script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	SaralBlog Multiple Input Validation CVE-2006-0345 CVE-2006-0346	7 (CVE-2006-0345) 2.3 (CVE-2006-0346)	Security Focus, Bugtraq ID: 16306, January 18, 2006
SleeperChat SleepterChat 0.3f and prior versions	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'Index.PHP' due to insufficient sanitization of the 'pseudo' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'chat_no.php' because arbitrary text can be inserted in the 'txt' parameter, which could let a remote malicious user post anonymous messages. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	SleeperChat Input Validation CVE-2006-0415 CVE-2006-0416	2.3 (CVE-2006-0415) 2.3 (CVE-2006-0416)	Security Tracker Alert ID: 1015525, January 23, 2006
Stringer Software Solutions My Amazon Store Manager 1.0	A Cross-Site Scripting vulnerability has been reported in 'search.php' due to insufficient sanitization of the 'q' parameter when performing a search, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	My Amazon Store Manager Cross-Site Scripting CVE-2006-0334	2.3	Secunia Advisory: SA18535, January 19, 2006

The electronic Farm Farmers WIFE 4.4 SP1 & SP2	A Directory Traversal vulnerability has been reported in the built-in FTP server listening on port 22003/tcp, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. An exploit script, DSR-farmerswife44sp1.pl.txt, has been published.	Farmers WIFE FTP Directory Traversal CVE-2006-0319	2.3	Secunia Advisory: SA18508, January 17, 2006
TopCMM Computing 123 Flash Chat Server 5.1, 5.0	A vulnerability has been reported when a variable is insecurely passed to an 'eval()' call, which could let a remote malicious user execute arbitrary code. Update available A Proof of Concept exploit has been published.	123 Flash Chat Remote Code Injection CVE-2006-0418	7	Security Focus, Bugtraq ID: 16360, January 24, 2006
Webspot WebspotBlogging 3.0	An SQL injection vulnerability has been reported in 'login.php' due to insufficient sanitization of the 'username' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Update available There is no exploit code required; however, a Proof of Concept exploit, WebspotBlogging.txt, has been published.	WebspotBlogging SQL Injection CVE-2006-0324	7	Secunia Advisory: SA18560, January 20, 2006
Zoph Zoph 0.x	SQL injection vulnerabilities have been reported due to insufficient sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. The vulnerabilities have been fixed in version 0.5pre1. There is no exploit code required.	Zoph SQL Injection CVE-2006-0402	7	Secunia Advisory: SA18563, January 23, 2006

[back to top]

Wireless Trends & Vulnerabilities

This section contains wireless vulnerabilities, articles, and malicious code that has been identified during the current reporting period.

- bluediving-0.3.tgz: Bluediving is a Bluetooth penetration testing suite that implements attacks like Bluebug, BlueSnarf, BlueSnarf++, BlueSmack, and has features such as Bluetooth address spoofing.
- Worldwide Hotspot List Tops 100,000 Mark: According to JiWire, the total number of hotspots listed in its directory is now 103,555. In 2005, the number of worldwide hotspots grew 87 percent. The three top countries for hotspots were the U.S., the United Kingdom and Germany. Last year, the three top countries were the U.S., the U.K. and South Korea.
- Cambridge prof warns of Skype botnet threat: According to a Cambridge professor, Voice-over-IP apps could be used to cloak networks of zombies and launch Denial of Service attacks.
- Four new Trojans on the loose: Antivirus companies are warning that four new Trojans are on the loose, three aimed at mobile phones and a fourth at PCs. The mobile phone worms are disguised as legitimate applications and spread via Bluetooth or multimedia messages and affect phones running Symbian. The computer worm spreads via e-mail and purports to offer pornography.

[back to top]

General Trends

This section contains brief summaries and links to articles which discuss or present information pertinent to the cyber security community.

- Nyxem Mass-mailing Worm: US-CERT is aware of a new mass-mailing worm known as Nyxem (CME-24). This worm relies on social engineering to propagate. Specifically, the user must click on a link or open an attached file.
- FBI publishes 2005 computer crime survey: An FBI survey provides statistics on the state of computer security attacks and defense technologies used by all sizes of organizations. Nine out of ten organizations experienced security incidents in the past year. Over 64% of respondents incurred a financial loss as a result of computer crime; however, only 9% reported these incidents to law enforcement. The United States and China top of the list as by far the worst offenders, together accounting as the source of more than half of all external intrusion attempts. The survey also reports that 44% of all reported intrusions were internal to the organization affected.
- Half-million PCs infected by e-mail virus: According to evidence from a web counter, a mass-mailing computer virus that is coded to delete files on February 3 may have spread to more than 500,000 servers. The virus that is known as the Blackmal.E or Nyxem.E virus, travels as an attachment to e-mail messages with suggestive subject lines such as "School girl fantasies gone bad" and "Re: Sex Video". The virus will completely compromise systems whose users open the attachment, attempting to disable security software and making extensive changes to the registry.

- Attackers To Go After 2006's Weakest Link: People: According to IBM's annual "Security Threats and Attack Trends Report", enterprises should expect a continued move toward stealthier, smaller, more focused attacks on their computer security, with the weakest link, workers' gullibility, increasingly the focus of hacker efforts.
- Kama Sutra Spoofs Digital Certificates: According to a Fortinet advisory, the Kama Sutra worm can fool Windows into accepting a malicious ActiveX control by spoofing a digital signature. The worm also goes by names such as Nyxem.e, MyWife.d, Grew.a, and Blackmal.e. It adds 18 entries to the Windows Registry to slip the ActiveX control by the operating system's defenses.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
2	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.
3	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
4	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
5	Sober-Z	Win32 Worm	Stable	December 2005	This worm travels as an email attachment, forging the senders address, harvesting addresses from infected machines, and using its own mail engine. It further download code from the internet, installs into the registry, and reduces overall system security.
6	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
7	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
8	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
9	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling anti virus, and modifying data.
10	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.

Table updated January 23, 2006

[back to top]

Last updated January 26, 2006